Phishing Malware vs Brazilian Banks: What each side is doing to raise the bar

Jacomo Piccolini
Security Academic Coordinator
IT Governance Academic Coordinator
Brazilian Research and Academic Network – RNP
Educational Team – ESR
www.esr.rnp.br
jacomo@rnp.br

Ivo Peixinho
Computer Forensics Expert
Head of the IT Division – DINF/CTI/DPF
Brazilian Federal Police
www.dpf.gov.br
peixinho.icp@dpf.gov.br
Brazilian home banking facts:

• Brazil started home banking operations in late 1990 with modem + proprietary software sent to users by floppy disks, remember those?

• Web access to home banking came around 1999 and fraud was limited until 2003 when phishing attacks started to become epidemic.

• Until 2007 almost all phishing attacks were based on simple fake web pages, sometimes with low quality, old images and old layout and non-working buttons.

• Since 2007 malware based attacks are the main door to collect user’s banking information but from time to time we do see a raise on fake banking pages, now with much better quality.
Brazilian home banking facts:

• Brazil has one of the largest banking operations on the world and is now heavily dependent on home banking and on ATM usage.

• Brazil is also one of the biggest Internet users population.

• Some official and non-official estimative says Internet banking fraud is generation losses around U$ 300,000,000 / year

• Wait one second .... that’s ONE billon in 3 years, that’s a lot of money ...
Raising the bar:

• First steps to defeat miscreants was based on virtual keyboards that were supposed to be immune to logging. They became standard to all banks in Brazil, and many run in Java
Raising the bar:

- Java can be easily decompiled

Base 64 Encoded Gifs

Decoded Output

Here is the decoded output of your Base 64 input:
Raising the bar:

• Java can be easily decompiled

Huh??

Embedded binary on Java code?

CPU and Disk data => Host identification (more on that later...)
Miscreants are hard to beat:

- Click logging start to kick in malware, it’s rudimentary but effective ...

... the hard work is to assemble all the clicks ...
Miscreants are hard to beat:

- Click logging start to kick in malware, it’s rudimentary but effective ...

Information can only be retrieved by a real person: 4/8 1/7 4/8 4/8 1/7 4/8 <ok>
Raising the bar:

• Second step used were to use two-way authentication with tan-code cards

• We call those “battleship” cards

• People carry them on wallets and even take pictures with cell phones 😊 not very safe

• And miscreants love those ...
Miscreants are hard to beat:

- Two way authentication with 70 entries, miscreants make you fill ALL positions 😊 before you can access the fake bank page 😊

... and people have time and patience to do that ...
Raising the bar:

- Browser plugins (g-buster)
Raising the bar:

- Browser plugins (g-buster)

"Infect" the machine before the miscreants do. G-buster monitors system for suspicious activity and reports back to the bank security team.
Miscreants are hard to beat: removing g-buster with Avenger tool

Thanks to Kaspersky
Miscreants are hard to beat: trading remover tools g-buster

If you have a g-buster killer or remover I will buy it or trade

Código fonte de kilador de gbuster, tem? eu COMPRO ou TROCO.
Se você tem um kilador de gbuster eu compro ou eu troco...
Deixa mensagem aqui mesmo que negociaremos por aqui ou pelo msn. abraços
Raising the bar: Tokens

• Tokens with timed password
  (few banks use those – only two?)
  • expensive
  • hard to maintain (helpdesk services)
  • users keep loosing, destroying, so on ...

• Tokens with digital certificates
  • not very used
  • user must buy one himself
  • uses Brazilian government PKI infrastructure (ICP-Brasil)
  • A3 certificates (hardware based)
Raising the bar:

• It started a new malware business - man in the “net” attack

User get infected

Malware check with database server – we have a new one!

Miscreant wait until his application play a song – we have a bank http request

Miscreant collect username/password and access the bank

Miscreant send a Token request to User

Token is sent to database

Miscreant receive the token

New song is played

Done!
Slide removed from original presentation
Slide removed from original presentation
Miscreants are hard to beat: Tokens pop-up
Raising the bar: Computer registration

• Bank of Brazil “computer registration” used to be like Microsoft WGA
  • if you change your HD or video card you need to register it again
  • if you make a new install you need to register it again
  • this was very effective for a short period of time ...
Miscreants are hard to beat: computer registration

... so Miscreants started to clone all information they need to defeat this ...
Raising the bar: SMS message for transaction commit

- Internet banking software send an SMS with a transaction validation to a pre-recorded cell phone number
- User must type SMS code to continue
- Used also to validate a new computer for the user
- Cheap way to have a “token”
- May be subject to SMS network congestion (bigger timeouts?)
Miscreants are hard to beat: Cell phone cloning by harvesting passwords of carrier websites

- Carrier stores use the Internet for registering new cell phones
- Store workers get bored and click on stuff they receive by email 😊
- With access, miscreants can “clone” cell phones and obtain SMS transaction codes
Miscreants are hard to beat: Cell phone cloning by harvesting passwords of operator software

Malware source (found on Google 😊)
Uses DELPHI language

Cell phone carriers
Miscreants are hard to beat: Cell phone cloning by harvesting passwords of operator software

```
A1.Mem1.Lines.Adc(A2.GIV);
A1.Mem1.Lines.Adc(IntToStr(Screen));
A1.Mem1.Lines.Adc('BEA>ESC0_');
A1.Mem1.Lines.Adc(Decry('k<öäÂ³vO!') + ': + [' -tl..exz + ''])
A1.Mem1.Lines.Adc(Decry('kRy 'çxyu') + ');
```
Raising the bar: Cellular registration – NEW

• This is new in the Brazilian Banking economy

  • Cell phone is a commodity – we have 180 million x 200 million population
  • Cost is transferred to end user – you use your phone
  • Different architecture – less malware (for now)
  • Have some issues – dead battery
    - no signal (inside a bunker)
    - network congestion (mia sms)

• Mobile will be the new desktop – FACT

  • Miscreants will target cell phones / technology / carriers
  • You will be kidnapped with your phone 😊
Miscreants are hard to beat: ATM skimmers are always present

Picture removed from original presentation
Miscreants are hard to beat: .pac files to change proxy configuration

... and the winner is ...

Miscreants, since this .pac file is online for more than two months ...

Sorry guys but #FAIL
Miscreants are hard to beat: hosts manipulation are common

This hosts file has ‘only’ 422 entries 😊
Defacing is still not a crime 😐 in Brazil

Picture removed from original presentation
Miscreants at large: Vídeo
What’s next?
What’s the next move?
What’s the solution?

Please THIS IS a JOKE:

This is NOT a JOKE: Miscreants will compromise WIFI routers to route traffic ... or any other kind of home user equipment to make this ...
Latest police operations on bank fraud

- **Operação espelho – 04/16/2009**
  - 10 search warrants on 4 states
  - Credit card cloning (goat sucker) and cash withdrawal fraud
  - Inside job – miscreants infiltrated inside a government bank
- **Operação trilha – 05/28/2009**
  - Greatest police operation on Internet bank fraud so far
  - 136 search warrants on 13 states
  - Multiple frauds – Trojans spread by email and cameras on ATM machines
  - Pictures of the miscreants (one was arrested on the US)
Latest police operations on bank fraud

- **Operação Nômade** – 06/04/2009
  - 20 criminals arrested
  - Goat suckers used for cloning of the magnetic strip of cards
  - Fake credit card billing machines for storing card information
  - Operation name (nomad) came from constant address changes from miscreants
- **Operação Contrafação** – 06/04/2009
  - 4 criminals arrested
  - Multiple operations – document forgery, credit card cloning and Internet fraud
  - Fake IDs, credit cards and computer software (trojans) found
- **Operação Clonagem** – 09/16/2009
  - Bank card cloning
  - Electronic devices for card cloning found with the criminals
  - Also R$ 4,000,00 in CASH 😊
Latest police operations on bank fraud

• Operação Ícaro – 03/04/2010
  • 4 states involved
  • Credit card cloning
  • Criminals used the cards to purchase products on the Internet, specially plane tickets
  • Use of social engineering – calling victims home to get card information
  • Selling of credit card numbers – from R$ 3,00 to R$ 150,00 depending on the limit

• Operação Neverland – 05/03/2010
  • Harvesting of bank passwords using trojans
  • Payment of bills using these passwords
  • This operation was a result of the “tentáculos” project
  • The leader of the group had a nickname of “Michael Jackson”
  • R$ 700.000,00 on financial loss
Latest police operations on bank fraud

- Operação RASTRO – 05/28/2010
  - Credit card cloning
  - 1,500 cards found with the criminals
    - Greatest card seizure EVER from the Federal Police
  - Money laundry – criminals buy stuff with cards and sells them with lower price
  - Group leader used the cards to buy construction materials for him to build his house 😊
  - Gang acquired R$ 1,500,000,00 on stuff
  - This picture is not his house 😊😊😊
Tentáculos project (2009 – 2010)

• Partnership between the Federal Police and Banks for obtaining Internet fraud information.
• Gathering of info from multiple banks and use of intelligence tools for correlation between frauds and criminals.
• Already resulted on one operation (neverland)
• Permanent group on the Federal Police focused on electronic fraud.
• Expected Result: reduction on 50% of frauds
Thanks – Questions to:

Jacomo Piccolini  
Security Academic Coordinator  
IT Governance Academic Coordinator  
Brazilian Research and Academic Network – RNP  
Educational Team – ESR  
www.esr.rnp.br  
jacomo@rnp.br

Ivo Peixinho  
Computer Forensics Expert  
Head of the IT Division – DINF/CTI/DPF  
Brazilian Federal Police  
www.dpf.gov.br  
peixinho.icp@dpf.gov.br